The Economic Impact of Security Breaches on Publicly Traded Corporations: An Empirical Investigation

Jesus Cardenas
Business/ IDS, UTEP, El Paso, TX, United States., jacardenas3@utep.edu

Adolfo Coronado
Information and Decision Sciences, University of Texas at El Paso, El Paso, TX, United States., adolfoc@utep.edu

Aurelia Donald
Information Systems and Decision Sciences, University of Texas at El Paso, El Paso, TX, United States., andonald@utep.edu

Fernando Parra
College of Business Administration, University of Texas at El Paso, El Paso, TX, United States., parra@utep.edu

M. Adam Mahmood
Information and Decision Sciences, University of Texas at El Paso, El Paso, TX, United States., mmahmood@utep.edu

The Economic Impact of Security Breaches on Publicly Traded Corporations: An Empirical Investigation

Jesus Cardenas
University of Texas at El Paso
jacardenas3@utep.edu

Adolfo S. Coronado
University of Texas at El Paso
adolfoc@utep.edu

Aurelia Nicholas-Donald
University of Texas at El Paso
andonald@utep.edu

Fernando Parra
University of Texas at El Paso
fparra@utep.edu

M. Adam Mahmood
University of Texas at El Paso
mmahmood@utep.edu

ABSTRACT

In a 2008 survey of 522 computer security professionals, the Computer Security Institute found an average reported cost close to $500,000 for those companies that experienced a financial fraud. A survey of potential cloud computing adopters show that security and privacy are the primary concerns for not using the cloud. The present research conducts an event study to investigate the impact of publicly announced security breaches on the market value of the breached companies. We utilize the cumulative abnormal returns, risk shifts, and volume changes to measure this impact. Our results show that the cumulative abnormal return due to a security breach is -.19%. We also found the mean risk factor increases by about 22 percent. Our results also show an abnormal trading volume of about 6%. None of the previous research studies in the information systems area has investigated the impact of security breaches on cumulative abnormal returns, volume changes, and risk shifts.

Keywords

Security breaches, event studies, abnormal returns, abnormal volume, and risk shifts.

INTRODUCTION

In an anonymous 2008 survey of 522 computer security professionals, the Computer Security Institute found an average reported cost of close to $500,000 for the companies that experienced a financial fraud (Richardson, 2008). Security breaches, by one estimate, affect around 15% of the companies' capitalization (Cashell, Jackson, Jickling and Webel, 2004). With the advent of cloud computing that "enables convenient, on demand network access to shared pool of computing resources (e.g., networks, servers, storage, applications, and services)" (NIST, http://csrc.nist.gov), privacy and security issues are expected to exacerbate. Cloud computing provides access to the data in an efficient manner especially without the start-up costs, but the challenge is to ensure that only authorized users gain access to it. In a survey of 572 business and technology executives, IBM found that 90 percent of the participants indicated that their companies were expected to pilot, adopt or implement cloud in three years (http://ibm.com/cloud-computing). In another survey of potential cloud computing adopters showed that security and privacy are the primary concerns for not using the cloud (Bruening and Treachy, 2009).

Security breaches have always been a problem, with or without cloud computing, for businesses in general and publicly traded companies in particular. Financial losses due to information security breaches have, however, always been difficult to measure due to the lack of methodologies for calculating actual losses incurred and the categorization of these breaches (Cavusoglu, Mishra, and Raghunathan, 2004; Mercuri, 2003). A few studies in the information security discipline produced mixed results in this area. Campbell, Gordon, Loeb, and Zhou (2003), for example, discovered significant market reactions to confidential data breaches (e.g., unauthorized access to credit card data) but no significant reactions to breaches that do not involve confidential data (e.g., denial of service attack). Cavusoglu, Mishra, and Raghunathan (2004) found that security breach announcements are negatively related to the market value of the announcing firms but a significant limitation of the their study, by the authors' own admission, relates to the categorization of breach types as attacks of any type. A study by Goel and Shawky (2009) revealed a significant negative impact of security breaches on the market value of the firm. Again,

incident details were not clear. Bolster, Pantalone, and Trahan (2010) found that only when the breach is announced in a major newspaper, the impact on the firm value is negative and significant.

In the present research, we focus on the economic impact of clearly defined security breaches on publicly traded companies using an event study methodology. In order to investigate the competing arguments concerning the economic impact of publicly announced information security breaches, one must clearly define these breaches and use a reliable and comprehensive technique to measure its impact. In the present research security violations are defined, to avoid any confusion between privacy and security breaches, using the National Institute of Standards and Technology (2007) guidelines, as any external, web-based act that results in violations of NIST security elements such as identification, authentication, authorization, integrity, non-repudiation, and confidentiality (Singhal, Winograd, and Scarfone, 2007). More specifically, we define security breaches, in the present research, as attacks that compromise the confidentiality and integrity of a firm's data and information assets (e.g., social security numbers, credit card numbers, bank account numbers, driver's license numbers, and identity theft).

The purpose of the present research is to empirically investigate the stock market reactions to security breaches on firms listed on one of the United Stock Exchanges (e.g., NASDAQ, NYSE, and AMEX) between the years 2002 to 2009 in terms of abnormal returns, abnormal trading volume changes, and abnormal risk shifts. None of the prior studies, to the best of our knowledge, have provided stock market reactions to security breaches in this comprehensive manner. All of these, we hope, will provide a clear picture of the effect of clearly defined security breaches on the market value of the breached companies and, in the process, will clarify some of the confusion in the area.

The rest of paper is organized in the following manners: the next section provides a literature review of event studies of security breaches. The third section develops the hypotheses used in the present research. The fourth section offers a description of the sample selection process and methodology used to analyze the data. The fifth section provides the results.

LITERATURE REVIEW

A number of previous research studies have examined cumulative abnormal returns from security breaches. The results from the previous studies in this area are, however, mixed. In this section, we first discussed some of the recent the studies that found significant and negative impacts from security breaches (Chen, Li, Yen and Bata, 2011; Gatzlaff and McCullough,2010; and Gordon, Loeb and Zhou, 2011) followed by those that did not detect any such impacts (Kannan, Rees, and Sridhar, 2007; Bolster, Pantalone, and Trahan, 2010; and Patel 2010).

Event Studies with Significant Results

Chen, Li, Yen and Bata (2011) explored the impact of information security breach events on the stock price of consulting firms that supplied the know-how and infrastructure to create, implement, and maintain those information systems that were hacked. The authors postulated that the market value of the IT consulting firms will also be negatively affected by the disclosure of IT security breaches. Using a sample of 83 breach announcements and a 2-day event window (0,1), the authors found that consulting firms had an average abnormal return of about 4% during a 2-day period around the announcements. The authors further determined that events involving extensive record breaches did hurt the stock prices of the IT consulting firms more than attacks with fewer records. Impacts of breach events on IT consulting firms were also stronger when technology and retail sectors were affected.

Gatzlaff and McCullough (2010), using a sample of 77 events of security breaches, found significant and negative cumulative abnormal returns on the stock prices of the breached companies. In addition, the authors ascertained that a negative relationship between the market reaction and firms that are less forthcoming about the details of the breach exists. Companies with higher market-to-book ratios also experienced greater negative abnormal returns associated with security breaches. Firm size and subsidiary status are, however, shown to mitigate the damaging effect of these breaches. Finally, the authors suggested that the attacks became more financially damaging in more recent years than in the past.

Another event study produced by Gordon, Loeb, and Zhou (2011), investigated the public announcements of information security breaches. The study included 121 security incidents that were announced in 5 specific newspapers: Wall Street Journal, New York Times, Washington Post, Financial Times, and USA Today. An event study was conducted using all 121 incidents first. The 121 breach incidents were then divided into two groups: 60 incidents were included in the pre-9/11 group and 61 were included in the post-9/11 group. The CAR was computed using a 3-day event window and 121 trading days before the event for both subgroups. Overall, the authors found that there was a significant negative impact of the breaches on

stock market returns of the breached firms. The authors further discerned that the breaches that happened before the 9/11 period caused a significant negative abnormal returns but the breaches that occurred after the 9/11 period did not show a significant impact.

Event Studies with Non-Significant Results

In addition to comparing different type of firms, some of the past researchers also conducted event studies based on different event windows. Kannan, Rees, and Sridhar (2007), for example, used 3-day, 8-day, and 30-day event windows around the breach announcements of 60 companies that reported a security breach in the New York Times or Wall Street Journal from 1997 to 2003. The market reaction to 102 security breach events was examined. Using the CARs computed over the aforementioned event windows, the authors found that none of the CARs were significant. The market reaction to security breaches was further investigated by analyzing the firm size, the type of attack, and the characteristic of the period of attack. Interestingly, the market reactions to confidentiality breaching attacks that were characterized as theft of credit card numbers, source codes, and unauthorized access, did not result in negative abnormal returns. The authors conceded these results could be due to the aggregation of all types of breached attacks.

Bolster, Pantalone, and Trahan (2010) conducted an event study that also combines both privacy and security breaches on a sample of 93 firms. Using event windows of (-1, 0), (-1, 0, +1), and (1, 30), and an estimation window of -301 to -46, overall the authors found no statistically significant and negative effect of security and privacy breaches on stock market returns of the affected companies. Interestingly, even the CARs of companies that suffered a loss from stolen data and social security numbers were not significant.

Patel (2010) also used an event study analysis to investigate the financial impact of publicly announced security breach announcements on 34 publicly traded companies listed on the DatalossDB organization. Using -3, ¬8, and -30 day event windows, the author found no significant and negative CARs suffered by the affected companies both in the short and long terms. The author stated that the results could be due to the small size of the sample used in the study.

The aforementioned literature review suggests that stock market reactions to publicly announced information security breaches are not conclusive. The present research aims to ascertain why this discrepancy exists. It is our opinion that this happened mainly for three reasons: first, in most of the past studies, the security and privacy breaches were not clearly defined. Second security and privacy breaches, in most cases, were combined. Third, abnormal volume changes and abnormal risk shifts that may be caused by these security breaches were not taken into consideration. Clearly the aforementioned discussion provides an impetus for conducting further research studies on the impact of clearly defined and publicly announced security breaches on the market value of publicly traded corporations.

The objective of the present research is to conduct an event study that addresses the aforementioned ambiguity by first clearly defining the security breaches. More specifically, we investigate the effect of clearly defined and publicly announced security breaches on the market value of breached companies in terms of abnormal returns. In order to provide more credence to our study, we also investigate the effect of security breaches in terms of abnormal volume changes and abnormal risk shifts. We expect the market to be rational and be able to distinguish between the types of lesser and more severe breaches and identify the potential losses based on the seriousness these breaches.

HYPOTHESES

Efficient Market Theory suggests that all public information is accounted for in a stock's current price. It is, therefore, expected that information security breaches in general will have a negative impact on stock prices. It is further assumed that the stock market reaction to a publicly announced information security breach on a publicly traded company will result in negative abnormal returns, abnormal volume changes, and abnormal risk shifts on its stock prices over a period of time before and after the breach announcements have been made. Unfortunately, the literature support for the impact of security breaches is not as unambiguous. Gordon at al. (2011), Chen et al. (2011), and Gatzlaff and McCullough (2010), as stated earlier, found significant and negative abnormal returns on stock prices for security breaches while Kannan et al. (2007), Bolster et al. (2010), and Patel (2010) noticed no significant and negative impact for these breaches on stock prices. These provide an impetus for testing this relationship.

We, therefore, propose the following hypothesis:

H1: Publicly announced and clearly defined information security breach incidents suffered by a company listed on one of the US stock exchanges will result in a loss in its market value as identified by negative cumulative abnormal returns on its stock.

An investor, before buying a stock, wants to know the levels of risk he or she is undertaking in purchasing the stock. Beta provides a value that represents the stock's volatility compared to the stock market. It is expected that if a company suffers a security breach the beta for its stock will be higher. Unfortunately, we find no research study in the information systems area that measures the risk shifts due to a publicly announced security breach. We have, therefore, borrowed one from the information privacy area and one from the studies conducted in the finance area to ground the following hypothesis. Nicholas-Donald, Matus, Ryu, and Mahmood (2011), in the information privacy area, found that betas for publicly traded companies with privacy breaches have significantly increased after the breach announcements have been made. Miihkinen (2010) ascertained, using OLS regression analysis on security breached companies listed on the Finnish Stock market, cumulative abnormal returns of these companies are negatively influenced by the quality of mandatory risk disclosures the companies must provide in its annual reports.

We hypothesize, based on the aforementioned discussion, the following hypothesis:

H2: A publicly traded US company that announces a security breach incident will experience increased risk as measured by its betas

Trading around earnings announcements should also be of interest to potential investors because it is systematically associated with post announcement returns (Garfinkel and Sokobin, 2006). Again, we find no research study in the information systems area that measures the volume changes for stocks due to a publicly announced security breach. We have, therefore, borrowed one from the information privacy area and one from a study conducted in the finance area to ground the following hypothesis. Nicholas-Donald et al. (2011) found, in the information privacy area, companies with privacy breaches suffer from significantly increased volume changes after the breach announcements have been made. Yun and Kim (2010) investigated the effect of changes in KOSPI 200 Index composition. The authors found that when a stock is added to the KOSPI Index, it's trading volume increases significantly during the event period and stays high even after the event has taken place. By the same token, trading volume decreases for stocks that have been deleted form the Index.

These lead to the following hypothesis:

H3: A publicly traded US company that announces a security breach incident will experience a decrease in its stock volume .

Sample Selection and Research Method

For the purposes of this study, a security breach event is defined as the first public disclosure of a breach of security in a major publication. The study covered such events that occurred between January 1, 2002 and December 31, 2008. Lexis/Nexis and the technology portals CNET and ZDNET were used to collect the publications because these cover the major U.S. newspapers and they are also highly regarded as sources of Information Technology news.

The events were then cross related to match only companies that were publicly traded in the U.S. markets. These events were further classified and filtered in accordance with the following criteria: a. only events associated with publicly traded companies that were listed on NASDAQ, AMEX, and NYSE were included; b. events that occurred around the time of another confounding event, such as a merger, acquisition, and earnings reports were eliminated; and c. only those events were included in the sample for which a precise date on which the public announcement of the security breach was made was available. We used the Compustat database to collect financial statement data and utilized the Center for Research in Security Prices (CRSP) database to gather information on stock prices and trading volume. The aforementioned rigorous screening process resulted in the selection of a total of 39 events of security breaches during the aforementioned time period.

In the present research we use three approaches to capture the effect of a breach on firm value. The market model is used that is grounded in the Capital Asset Pricing Model (CAPM) which is widely used and accepted in the finance and accounting

literatures. The estimation of expected returns is based in an ordinary least squares (OLS) regression. In this regression, the independent variable is the market index for time (t), and the dependent variable is the return of security (i) at time (t) as shown in the following Equation 1.

$$R_{i,t} = \alpha_i + \beta_i R_{m,t} + e_{i,t} \quad (1)$$

where, $R_{i,t}$ is the return for firm i on day t, $R_{m,t}$ is the return on the market portfolio on day t, α_i and β_i are parameters in the model, and $e_{i,t}$ is the disturbance term.

A minimum of 120 trading days for the estimation window is acceptable [32]. In the present research, an estimation window of at least 250 trading days (a full calendar year) is used. The estimation window begins 251 trading days prior the event day (t=0). All of the 38 sample firms have the full 250 trading days of return data as required. As proxy of the market portfolio (market index), the CRSP value-weighted index, is used. After the regression parameters are estimated, the abnormal returns are calculated by subtracting expected returns from the observed returns (see Equation 2).

$$AR_{i,t} = R_{i,t} - (\hat{\alpha}_i + \hat{\beta}_i R_{m,t}) \quad (2)$$

It is possible that the markets do not fully incorporate information instantaneously; therefore, the used of a multi-day event window is required. During this event window abnormal returns are accumulated to form Cumulative Abnormal Returns (CAR). In the present research the event window consists of 3 trading days surrounding the event announcement date (see Equation 3).

$$CAR_i = \sum_{t}^{t+n} AR_{i,t} \quad (3)$$

Two variations of CAR are computed for robustness. First, CAR is winsorized. Winsorization is the process of replacing extreme observations with the closest CAR in the arranged list of CARs. For example, the smallest CAR is replaced by the second to the smallest CAR. This process eliminates the influence of outliers in the results. Second, CAR was transformed by taking the natural log of (CAR + 1).

The one-factor model (see Equation 1) was also used to estimate the firm's beta both pre (day -251 to day ¬1) event date and as post (day +1 to day +251) event date. The post-event beta is divided by the pre-event beta (see Equation 4), providing a standardized beta ratio. This ratio should be equal to one if the event had no impact on the firm's risk, a ratio lower than 1 is a reduction of risk and a ratio greater than one should be interpreted as an increase of firm's risk. Because betas consider the correlation of returns to the whole financial market, there is no bias for the selection of those entities that were breached, for if the whole market presents a down trend, the betas will take this trend into consideration.

$$\beta_{ratio,i} = \frac{\beta_{post,i}}{\beta_{pre,i}} \quad (4)$$

The abnormal volume is used as a third measure of abnormal activity in the firm's equity surrounding the security breach announcement day. In this capacity, two different techniques were used to estimate abnormal trading volume changes. The technique used in the present research is based in the work of Yun and Kim (2010) and Beneish and Whaley (2002). The authors scaled the average event window daily volume by the 60-day daily average pre-event volume. If this ratio results in a normal daily trading volume, the ratio is expected to be equal to one. Any deviation from 1 is considered to be abnormal trading volume.

RESULTS

Table 1 provides the results for H1. Our analysis of 39 security breaches provided an average CAR of −0.1915439%. This negative abnormal return is, however, not statistically significant at an acceptable p-value.

N	Mean	t-Value	Pr > |t|
39	-0.0019154	-0.2441	0.8085

Table 1: The Means Test for Cumulative Abnormal Returns

The risk shift was observed by analyzing the changes on pre-and post-betas. We used the single-index CAPM model, as explained by Yun and Kim (2010), to calculate calculate pre- and post-betas. Both, the pre- and post-betas were calculated using the 250 trading days surrounding the event announcement day. The means test results for the prior-and post-event betas are shown in Table 2. Our analysis shows that the beta of firms with security breaches has significantly increased after the security breach announcements. This risk increase is observed in the beta ratio (see Equation 4), where the expectation for normal trading volume is a ratio of 1. In this case, the ratio is over 1, indicative of an increase in risk as measured by betas' shifts.

N	Mean	t-stat (p-value)
38	1.15252	12.826 (3.459e-15) (Pre-event beta)
38	1.14174	14.0218 (2.2e-16) (post-event beta)
38	1.22307	6.68 (7.594e-08) (beta ratio)

Table 2: The Means Test for Beta

Next, we analyze the abnormal trading volume experienced by the breached firms. In the present research we follow a technique based in the work of Beneish & Whaley (1996) and Yun and Kim (2010) to calculate the abnormal trading volume for each of the breached companies. As previously mentioned, this method uses the average trading volume for the pre-event 60 trading days and this is compared with the volume of the event window [-1, 0, +1] for each company. Using this technique, we observed that the breached firms experienced a significant abnormal trading volume of about 5% during the event window (see Table 3).

N	Mean	t-stat (p-value)
39	1.05862	9.7278 (9.681e-12)

Table 3: Abnormal Trading Volume

DISCUSSION

The results of the present research show that publicly announced security breach announcements make businesses loose market value. These negative abnormal returns are not, however, significant. Our research findings are aligned with Gordon at al. (2011), Chen et al. (2011), and Gatzlaff and McCullough (2010). We believe with a larger sample, the results will be both significant and negative. We are in the process of increasing the sample size. We will ensure that in the larger sample companies with multiple breaches are not included.

Our results demonstrate that the firms have, with publicly announced security breaches, experienced a significant increase in risk as measured by their betas. The average cost per event of the breached companies was an average reduction in the market returns of -.19%, so we consider that investing in security prevention hardware and software is worth for companies as they can be spending much more money than the cost of preventive measures if they do not protect themselves. Again, we are unable to compare our results with security studies in the information systems area since none are available. Our results do, however, allow us to agree with Nicholas-Donald at al. (2011) in the information privacy area and Miihkinen (2010) in the finance area when they found that a negative event suffered by a company effects the company's beta negatively.

Our results also confirm that the security breached firms had experienced cumulative abnormal volume. Again, none of research studies, in the information systems area, has investigated the abnormal volume changes around the time security breach announcements were made public. Our results do, however, allow us to agree with Nicholas-Donald et al. (2011) in the information privacy area and Yun and Kim (2010) in the finance area when they stated that a negative or positive event encountered by a company results in an increase in its abnormal volume by a company results in an abnormal volume.

CONCLUSION

The present research contributes to the information security area in a number of ways: first, it clearly defines information security using the well-accepted NIST standard. In the process, we believe it has diminished the ambiguity that is present in the information security and privacy area. Second, it then conducts an event study, using the clearly defined information security breaches, on a sample of companies that went through a publicly announced security breaches to generate abnormal returns. Third, in order to provide more credence to our study, we also investigate the effect of security breaches in terms of abnormal volume changes and abnormal risk shifts. We hope by completing the aforementioned, we were able to move the information security breach area a little forward.

REFERENCES

1. Acquisti, A., Friedman, A., and Telang R. (2006). Is there a cost to privacy breaches? An Event Study. *Twenty Seventh International Conference on Information Systems*, Milwaukee 2006, 1-23.
2. Bali, R. and Francis, J. C. (2010). Trading volume around ex-dividend days. *Applied economic letters*, 18, 8, 769¬772.
3. Beneish, M.D., and Whaley, R.E. (2002) S&P 500 Index Replacements, *The Journal of Portfolio Management* (Fall 2002), 29, 1, 51-60.
4. Bolster, P.J., Pantalone, C.C., and Trahan, E.A. (2010) Security Breaches and Firm Value , *Journal of Business Valuation and Economic Loss Analysis*. 5, 1, 1.
5. Bruening, P., and Treachy, B. (2009) Cloud Computing – data protection concerns unwrapped, *Privacy and Data Protection PDP*, 9,3, 1-3.
6. Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003, April) The economic cost of publicly announced information security breaches: empirical evidence from the stock market, *Journal of Computer Security*, 11, 431-448.
7. Cashell, B., Jackson, W., Jickling, M., and Webel, B. (2004), The economic impact of cyber-attacks*, Congressional Research Service Report for Congress*.
8. Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004) The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers, *Int. J. Electron. Commerce*, 9, 70-104.
9. Chen, J. V.; Li, H. C., Yen, D.C., and Bata, K.V.. (2012) Did IT consulting firms gain when their clients were breached?, *Computers in Human Behavior*. 28, 2, 456–464.
10. Garfinkel, J.A., and Sokobin, J. (2006) Volume, Opinion Divergence and Returns: A Study of Post-Earnings Announcement Drift, *Journal of Accounting Research*, 44, 1, 85–112.
11. Gatzlaff, K. M. and McCullough, K.A. (2010) The effect of data breaches on shareholder wealth, *Risk Management and Insurance Review*,13,1, 61-83.
12. Goel, S., & Shawky, H. A. (2009) Estimating the market impact of security breach announcements on firm values, *Inf. Manage*., 46, 404-410.
13. Gordon,L. A.; M. P. Loeb; L. Zhou (2011) The impact of information security breaches: Has there been a downward shift in costs?, *Journal of Computer Security*, 19,1, 33-56.
14. Kannan, K., Rees, J., & Sridhar, S. (2007) Market Reactions to Information Security Breach Announcements: An Empirical Analysis, *Int. J. Electron. Commerce*, 12, 69-91.
15. Mercuri, R.T., (2003) Analyzing Security Costs, *Communications of the ACM*, 46, 6, 15-18.
16. Miihkinen, A. (2010) The Usefulness of Firm Risk Disclosures under Different Firm Riskiness, Investor Interest, and Market Conditions? Evidence from Finland, (December 15, 2010). Available at *SSRN: http://ssrn.com/abstract=1725582*
17. Nicholas-Donald, A.; Matus, J.F.; Ryu, S.; and Mahmood, A.M., (2011) The Economic Effect of Privacy Breach Announcements on Stocks: A Comprehensive Empirical Investigation, *AMCIS 2011 Proceedings* -All Submissions. Paper 341. http://aisel.aisnet.org/amcis2011_submissions/341.

18. Patel N. (2010) The effect of IT hack announcements on the market value of publicly traded corporations*, Duke Journal of Economics*. Vol. XXII, Spring 2010.

19. Richardson, R. (2008) 2008 CSI Computer Crime and Security Survey, *Computer Security Institute*.

20. Singhal, A., Winograd, T., and Scarfone, K., (2007) Guide to secure web services (NIST SP 800-95), *Technical report, National Institute of Standards and Technology (NIST)*.

21. Yun, J. and Kim, T.S., (2010) The effect of changes in index constitution: Evidence from the Korean stock market, *International Review of Financial Analysis*,19, 4, 258–269.

PERMNO event_date	car	beta_before	beta_after	vol_ratio
84165 2002-11-27	0.0164497799	1.653495527	1.4544536817	1.2603432565
11754 2004-06-22	0.043821146	1.0382474236	0.9577172881	0.7420745614
59408 2005-02-26	-0.0001891078	0.8273163902	0.7367673931	1.1375861126
85072 2005-04-15	-0.0525586928	0.970546406	1.2986108651	1.1137995629
87033 2005-04-15	0.0231215417	0.6890140923	0.5790089284	0.9789229088
59408 2005-10-07	0.0371624972	0.8761993986	0.7964312143	0.9510035289
19561 2005-11-18	0.0105816389	0.9307826239	1.1206830091	0.9753106488
55976 2005-12-12	0.0354918956	0.7399178276	0.776057643	0.8437598107
27888 2006-05-19	0.0220308021	1.0503596642	0.7557148693	1.2171837844
81481 2006-08-01	0.0819769271	0.8003541153	1.1929306555	1.1420973519
80320 2006-08-28	-0.0250297692	1.0059553388	0.7731468614	0.7404327053
12106 2006-10-14	0.0395168856	0.0370693628	-0.0010828277	0.6568808303
80913 2006-11-03	-0.0813466385	0.8096941583	0.5973081232	1.2781603585
59408 2006-12-22	0.0056591714	0.7496176145	1.1114268987	0.933654242
84342 2007-01-12	0.0457464989	2.1374224999	1.2077108499	0.9251983953
64653 2007-01-29	0.0285718263	0.9182891213	1.344822993	1.0984194348
10874 2007-02-16	0.0113635557	1.1046646899	1.2222901583	0.974720196
27828 2007-05-07	0.0503901542	0.8999586858	1.0035428026	1.0644727184
77679 2007-05-21	-0.0077084789	1.5017670348	1.3928084926	1.3330023803
91282 2007-08-09	0.0700011407	1.9446096526	1.1926415235	1.1326079153
70519 2007-09-21	-0.0223891773	1.1755139052	2.3715604675	0.8918017222
27888 2007-11-07	0.0387039089	0.9500913144	1.0674707387	1.4473206358
70519 2008-01-25	0.13556217	1.3806605964	2.1501655204	1.4007074206
89217 2008-03-31	0.0027180523	0.9758446356	0.8529771823	0.7086635303
89179 2008-04-08	0.1266293277	0.1391072055	0.8820360542	0.8576936495
89179 2008-04-16	0.0938246888	0.1769614473	0.878163991	0.8172128726
49373 2008-06-04	-0.0058858274	0.955876884	0.9070609694	0.6094426462
36346 2008-06-10	-0.0938731477	2.0990426528	1.5156687728	1.2797380615
77668 2008-11-06	0.1791036761	0.9908162389	0.7470543088	1.1088715964
75937 2008-11-26	0.0963846885	1.0670867461	1.0603639477	0.8979599285
92355 2008-12-29	0.0273382973	1.9237996538	2.8120190143	0.0396183748
90833 2009-01-20	-0.5059123845	0.9869173134	1.2057922762	4.6891469095
89410 2009-02-03	-0.1562431309	0.7600427782	0.7702967675	1.2835155212
86819 2009-05-12	-0.2739510446	1.7559313259	1.1922208263	0.5629983633
86819 2009-05-19	-0.0473154802	1.7495251507	1.3557063281	0.4507519861
59408 2009-08-11	0.1133015548	2.2976496503	1.5228814132	0.7188343051
81055 2009-09-06	-0.0375050607	1.9852217622	1.5374426167	0.7029601009
49656 2009-10-28	-0.0144829275	1.7406643926	1.0443672483	1.2606000382

Appendix A: Research Variables